National Supervisory Control and Data Acquisition Test Bed

www.inl.gov

INL cyber researcher Jared Verba reviews circuit breaker settings on a power grid SCADA system.

Massive. Interconnected. Essential. These words describe the nation's critical energy infrastructures ranging from systems that light cities to networks that deliver oil and gas. Owned privately, but used publically, these complex, interdependent systems affect every person in each county, community, and parish in the country. And increasingly, the supervisory control and data acquisition (SCADA) systems that monitor and manage them are susceptible to malicious cyber attacks.

These attacks have been used to disrupt power equipment in regions outside the U.S. In at least one case, the disruption caused a power outage affecting multiple cities. Nation-states are also actively targeting utility computers. But ongoing research at Idaho National Laboratory (INL) is working to improve SCADA security and design more resilient control systems.

Since 2004, INL has been a significant contributor to the Department of Energy's broad National SCADA Test Bed (NSTB) program. This national research initiative was developed to help private utilities improve the resilience of control systems associated with energy sector critical infrastructure. Researchers from national laboratories, private industry, and universities collaborate to conduct detailed vulnerability assessments of SCADA systems, communications protocols, and third-party security products. The data collected is used to develop recommended protection strategies for system owners and manufacturers.

At INL, full-scale, industry-provided SCADA systems undergo regular cyber analysis by experts widely recognized for securing control systems. The laboratory also conducts onsite assessments and training at electricity transmission, generation, and oil and natural gas facilities to better understand real-world installations and provide mitigation strategies to owners and operators. Assessments are backed up by immersive training courses that teach owners and operators about emerging cybersecurity techniques and malware trends.

Quick Facts

- NSTB is a collaborative DOE initiative for securing SCADA and energy-related control devices.
- Five national laboratories and more than a dozen industry partners contribute to the program.
- Industry support and participation is encouraged during assessments, training, and implementation.
- SCADA systems from vendors with greater than 85 percent of the energy market have been assessed.

For More Information

Dave Kuipers
(208) 526-4038
david.kuipers@inl.gov

Idaho National Laboratory